Homeland
Security

DHS 4300A

Sensitive Systems Handbook

Attachment C

Information Systems

Security Officer (ISSO)

Designation Letter

Version 11.0

August 5, 2014

Protecting the Information that Secures the Homeland

This page intentionally blank

DHS Information Systems Security Officer (ISSO) /

Alternate Information Systems Security Officer (AISSO) Designation

The following person is designated as the □ ISSO / □ AISSO for the _____ (major application or general support system, as appropriate)

Name	
DHS Component	
Title	
Office	
Telephone Number	
E-mail Address	

Affiliation (select one)

□ DHS Employee.

□ DHS Support Contractor. If support contractor, provide name of contracting company: _____

Clearance

□ ISSO has been granted a Secret clearance (minimum)

Designating Official (System Owner, Senior Site Manager, or ISSO, as appropriate)

Name: _____   Title: _____

Signature: ____Date: _____________________

Review and Approval (by the Component Chief Information Security Officer or delegate)

Name: _____ Title: _____

Signature: ____   Date: ____________________

Comments: _____

ISSO / AISSO Acknowledgment of Responsibilities

I, ______________________ (print name), have been formally designated an □ Information Systems Security Officer (ISSO) / □ Alternate Information Systems Security Officer (AISSO) for the _______________________________________ (major application or general support system, as appropriate). I understand that I am responsible for coordinating information technology security regulations and requirements, as described in appropriate security policy publications and handbooks, including the following:

Ensuring that security requirements for the major application or general support system with which I am involved are being or will be met.

Ensuring that requests for certification and accreditation of computer systems are completed in accordance with the published procedures.

Ensuring that protective measures such as deadbolt locks on doors, placement of electrical wiring, etc. as countermeasures for physical security threats, are in place.

Ensuring compliance with all legal requirements concerning the use of commercial proprietary software, e.g. respecting copyrights and obtaining site licenses.

Maintaining an inventory of hardware and software within the program and development offices or field site facility.

Coordinating the development of a Contingency Plan and ensuring that the plan is tested and maintained.

Ensuring that risk analyses are completed to determine cost-effective and essential safeguards.

Ensuring preparation of security plans for sensitive systems and networks.

Attending security awareness and related training programs and distributing security awareness information to the user community as appropriate.

Reporting IT security incidents (including computer viruses) in accordance with established procedures.

Reporting security incidents not involving IT resources to the appropriate security office.

Providing input to appropriate IT security personnel for preparation of reports to higher authorities concerning sensitive and/or national security information systems.

DHS Component:
____

Office: _______________________________________Telephone Number: _______________

Signature ____ Date ____________________________